## **Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application:

## **Listing of Claims:**

1. (Currently Amended) In a public key encryption system, a method for selecting a current secret key to be used to encrypt a message, the method comprising:

determining whether a new secret key is required,[[;]]wherein determining whether a new secret key is required further comprises:

determining whether a previous message has been sent to a recipient;

if a previous message has not been sent to the recipient, determining that a new secret key is required; and

if a previous message has been sent to the recipient:

retrieving counter data from a local data store; and

comparing the counter data to a reuse criterion selected from a plurality of reuse criteria, wherein the selected reuse criterion comprises a maximum number of bytes of message data and the counter data comprises a cumulative number of bytes of message data previously sent using an associated reusable secret key;

if the counter data satisfies the selected reuse criterion, determining that a new secret key is not required; and

if the counter data fails to satisfy the selected reuse criterion, determining that a new secret key is required;

if a new secret key is required:

generating the new secret key;

generating a new encrypted secret key by encrypting the new secret key using a public key associated with [[a]] the recipient of the message;

storing in [[a]] the local data store the new secret key as a reusable secret key, the new encrypted secret key as a corresponding reusable encrypted secret key, and counter data associated with the reusable secret key; and

selecting as the current secret key the new secret key; and if a new secret key is not required:

## Serial No. 10/033,705

retrieving from the local data store a reusable secret key and the corresponding reusable encrypted secret key;

updating the counter data associated with the reusable secret key in the local data store; and

selecting as the current secret key the reusable secret key.

- 2. The method of claim 1, further comprising storing in the local data store state information associated with a cryptographic algorithm in which the reusable secret key is applied.
  - 3. (Canceled)
- 4. (Currently Amended) The method of claim 1[[3]], wherein the <u>plurality of reuse eriterion criteria comprises comprises a maximum number of messages and the counter data comprises a cumulative number of messages previously sent using the <u>associated reusable secret key.</u></u>
  - 5. (Canceled)
- 6. (Currently Amended) The method of claim 1[[3]], wherein the <u>plurality of reuse</u> eriterion <u>criteria comprises comprises</u> a maximum amount of elapsed time and the counter data comprises an amount of elapsed time since the <u>associated</u> reusable secret key was generated.
  - 7. The method of claim 1, further comprising: encrypting the message using the current secret key; and sending the encrypted message and the encrypted secret key.
  - 8. (Canceled)
  - 9. (Canceled)